

**INFORMATION GOVERNANCE ANNUAL REPORTS 2020/21**

<b>Trust Board</b>	<b>Item: 13</b>
<b>Date: 26 January 2022</b>	<b>Enclosure: J</b>
<p><b>Purpose of the Report:</b></p> <p>To present the IG annual report for discussion prior to submission to the Trust Board.</p> <p><u>Executive Summary</u></p> <p>This report covers the financial year 2020/21. Due to Covid-19 pandemic, the Information Governance Committee (IGC) did not meet as often as would be expected and other challenges related to the pandemic were experienced by the Information Governance Team in executing their duties.</p> <p>Highlights</p> <ul style="list-style-type: none"> <li>• The Trust meets national data quality targets.</li> <li>• Kingston Hospital FT templates are being used by other organisations across SW London to meet statutory requirements.</li> <li>• Kingston Hospital FT chaired the South West London Connecting your Care (CyC) IG Group, which successfully delivered Phase 2 of CyC and helped to put in place pan-London sharing of Acute and GP information under the Control of Patient Information Notice (COPI). The project was nominated for a National SIGNs (IG) award.</li> <li>• The Trust was at the core of the South West London Covid-19 IG Group which reviewed and approved 78 Data Privacy Impact Assessments to enable the flow of patient information to aid in treatment and control of the virus (over the two-year period of the pandemic so far).</li> <li>• Privacy Notice continues to be updated to include new uses of information. A second Covid-19 Privacy Notice has also been published.</li> <li>• Compliance with the National Data Opt-out has been implemented.</li> </ul> <p>Challenges</p> <ul style="list-style-type: none"> <li>• Covid-19 Pandemic increased the IG workload in terms of information sharing and producing Data Privacy Impact Assessments whilst also complicating Freedom of Information and Subject Access Requests due to staff sickness and redeployment.</li> <li>• Freedom of Information Requests – In 2020-21 the Trust received 553 requests with a response rate of 61.84% within 20 working days. The 2020-21 decrease was due to both staff sickness within the department and sickness and redeployment elsewhere in the Trust.</li> <li>• Versions 3 of the Data Security and Protection Toolkit was rated as 'Standards not fully met – plan agreed'. Subsequently the wording was changed by the Toolkit to "Approaching Standards Met"</li> <li>• Further IG SIRIs (Serious Incidents Requiring Investigation)</li> </ul>	
<p><b>For: Information</b> <input checked="" type="checkbox"/> <b>Assurance</b> <input type="checkbox"/> <b>Discussion and input</b> <input checked="" type="checkbox"/> <b>Decision/approval</b> <input type="checkbox"/></p>	
<b>Sponsor (Executive Lead):</b>	Sam Armstrong, Director of Corporate Governance
<b>Author:</b>	<i>Janice Sorrell, Head of Information Governance</i>
<b>Author Contact Details:</b>	020 8973 5292 Janice.Sorrell@nhs.net
<b>Risk Implications – Link to Assurance Framework or Corporate Risk Register:</b>	Report identifies significant risks and actions taken

<b>Legal / Regulatory / Reputation Implications:</b>	Regulatory and reputational implications
<b>Link to Relevant CQC Domain:</b> Safe <input checked="" type="checkbox"/> Effective <input checked="" type="checkbox"/> Caring <input type="checkbox"/> Responsive <input type="checkbox"/> Well Led <input type="checkbox"/>	
<b>Link to Relevant Corporate Objective:</b>	Strong foundations - good governance
<b>Document Previously Considered By:</b>	Information Governance Committee
<b>Recommendations:</b>	
The EMC is asked to review and approve this report prior to its submission to the Trust Board	

# Information Governance Committee Annual Report

## 1. Introduction

It has been both a busy and challenging year for information governance related activities. The following reports on the period 1<sup>st</sup> April 2020 to 31<sup>st</sup> March 2021. It is worth noting that the re-organisation of the IG Team to take on Subject Access Requests and the challenges presented by Covid-19 – both to the Team and wider Trust staff who needed to provide the information required – has contributed to poorer results in the period when compared to the previous year.

## 2. Principal Activities

The following points capture the key activities not presented elsewhere in the report.

**Data Security and Protection Toolkit version 3** – The Trust completed the Toolkit in 2020/21 with a rating of "Standards not fully met – plan agreed". Subsequently, the Toolkit has changed the wording to "Approaching Standards Met". Although the Trust has broad compliance across all ten assurances standards of the Toolkit version 3, it did not meet all Assertions, which was also the case in the previous year.

The Trust submitted improvement plans for ten IM&T Assertions, however a major challenge continued to be achieving the target 95% annual training standard.

**Training** – The Trust did not meet the NHS Digital target of 95% of all staff being trained in information governance annually. For version 3 of the Data Security and Protection Toolkit in 2020/21, the Trust achieved 84.55% (compared to 92.27% the previous year).

The training is available through the Electronic Staff Record Portal and this system sends out automatic reminders from 3 months before training is due to be re-taken. In addition, there have been various global emails regarding training and also targeted emails from the Head of Information Governance to those out of compliance. The latter were suspended when the hospital was especially busy due to Covid-19, which has likely affected the final results. Trusts struggle with having staff complete the training every year, and we are planning further promotion of the need to complete the training to our staff.

**Data Protection Act / Access to Health Records Subject Access Requests (SARs)** – The statutory timeframe to complete a request is one month, however the Trust has adopted a standard 28-calendar-days. The majority of these requests in-year were handled by the Health Records Team, however the process was passed to the IG Team from January 2021. The Assisted Conception Unit and Radiology Department also complete SARs. The transfer of SARs to Information Governance had some setbacks, including a lack of space, computers and equipment, and staff which have now been mostly rectified. We are fortunate to have an experienced member of staff transfer from the Health Records Department, and have also successfully recruited to a second Subject Access Officer role. The delays led to a backlog of requests, which the Team has been working through.

Figure 1 – SARs combined figures from health records, IG and Assisted Conception

Month	No. requests	Completed in 28 days	Percentage in 28 days
Apr	69	64	92.80%
May	91	78	85.70%
Jun	92	85	92.40%

Jul	146	120	82.20%
Aug	82	63	76.80%
Sep	160	104	65.00%
Oct	54	30	55.60%
Nov	114	43	37.70%
Dec	113	35	31.00%
Jan	122	47	38.50%
Feb	95	30	31.60%
Mar	86	31	36.00%
	1224	730	59.64%

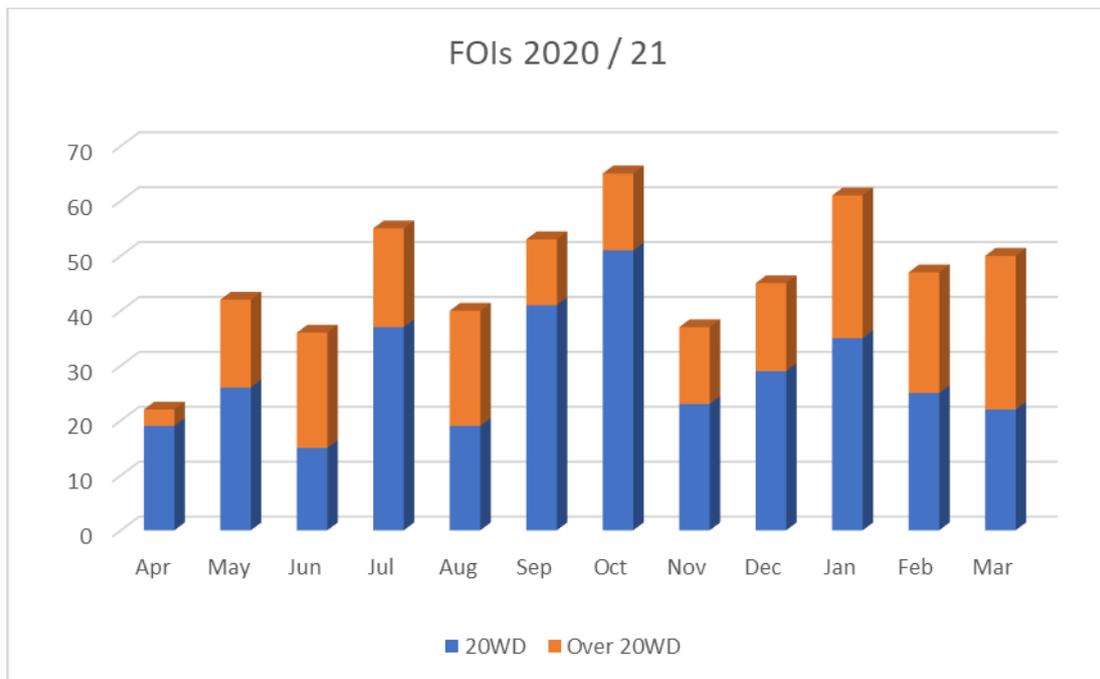
Radiology had a total of 1433 requests and completed an average of 99.86% within the time.

**Data Quality** – The Data Quality (DQ) Group is being reconfigured and re-established under new terms of reference. However, the Information Services Department continues to provide validation and other reports across the Trust. The IM&T Application Support Team continues to make improvements to “harden” the Electronic Patient Record to make it less likely to make data quality mistakes.

**Data Accreditation** – The Trust met national data quality targets, such as use of NHS number (i.e. wherever a patient has an NHS number we have it on their record). The Information Services Department, within Business Intelligence, provided a service catalogue of data quality reports which were available and in use across the Trust. Many of these reports were readily available through the Trust Intranet in Disco+ reports. This Department also strove to maintain and improve data quality through improving practice by users. There was further work on reporting of data quality issues to the initial point of creation to support the Trust initiative of getting the data right first time. The department also fulfilled data requests to support the Trusts efforts with the pandemic.

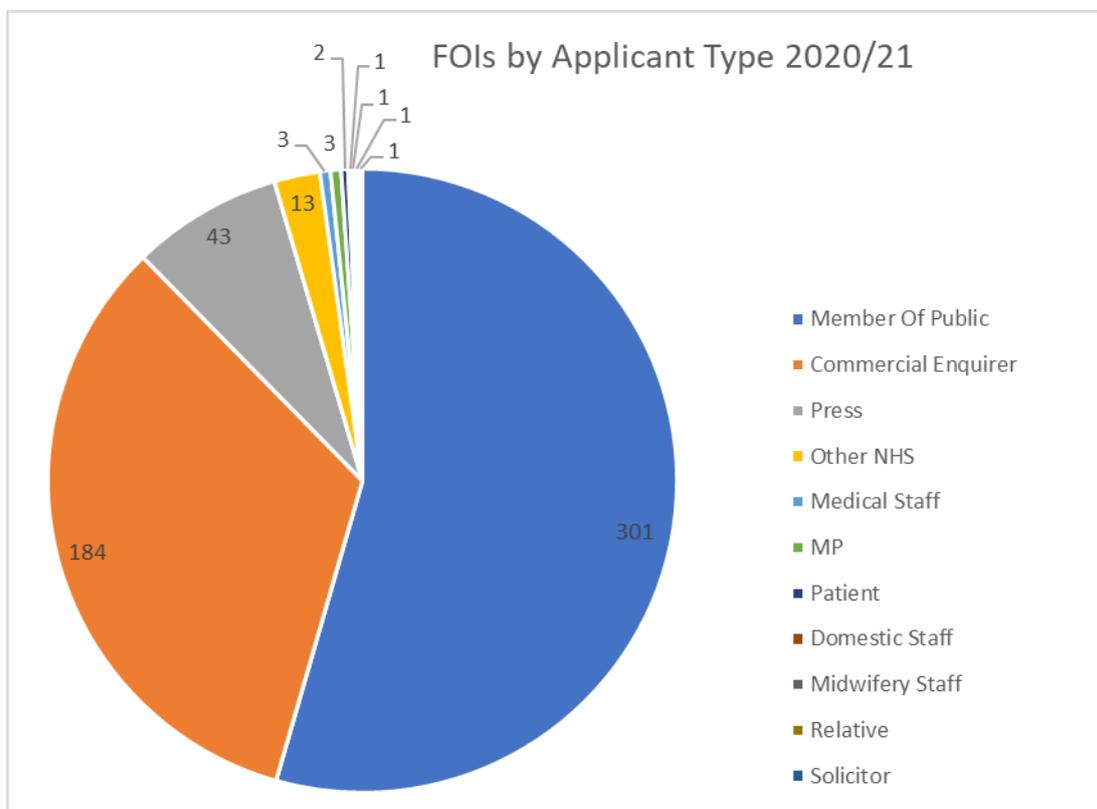
**Freedom of Information (FOI)** – Trusts are required to respond to FOIs within 20 working days. In 2020/21, the Trust received 553 requests and averaged over the course of the year to respond to 61.84% within the 20 working days (compared to 82.62% in 2019/20). Much of the decline in performance appears to be due to sickness in the department, as well as sickness, redeployment and other Covid-19 related pressures in the other departments where information is sourced. Also, while the number of requests fluctuates over the years, the complexity and size of individual requests continues to increase; individual requests are larger and require information to be collated from multiple departments. During the year, the Team has successfully recruited a second Information Governance Assistant. The ICO had stated during the pandemic that although they cannot formally alter the expected response protocols, they were understanding of the pressures NHS organisations were under during the period.

The following table demonstrates the number of FOIs received over the course of 2020/21 and the performance of achieving the 20-day requirement against not achieving this.



The following table demonstrates the FOIs received by applicant for the information.

While the majority are assumed to be categorized as general public (and this group may still include those represented in others categories that could not be identified at the time of requesting) it is interesting to note the high number of requests from commercial providers and the press; the third highest group after those two was MPs or their assistants.



The following table demonstrates the top FOIs by Category 2020/21

2020 / 21	
Category	No of FOIs
Corona Virus	70
IT Infrastructure / Software E	64
Staff Information	61
Drug Information - No Pts Pres	39
Statistics E.G LoS, Nos Proceed	38
Agency And Bank	30
Contract Information	18
Equipment	16
Service Performance	16
Finance	15
Policies / Procedures / Guidel	15

**Contributing across SWL: Connecting your Care and panLondon Acute and GP Sharing**

The Trust is actively engaged with, and made a major contribution to, the South West London Information Governance Group, chaired by the Trust’s Head of Information Governance, and has helped to further develop the GDPR compliant Overarching Information Sharing Agreement, which sets out the framework within which Purpose Specific Information Sharing Agreements must comply. This has been passed by the Group, the LMC (Local Management Committee) and legal review. The Group has also adopted the Kingston Hospital Tier 2 Purpose Specific Information Sharing Agreement Template (PSISA) which was updated to be GDPR compliant. This work has been done to facilitate a Health Information Exchange (HIE) across the whole of South West London, to have information from the Acute Trusts, Mental Health Trust, GP practices, Adult Social Care, Pharmacies (pilot sites) and Care Homes (also pilot sites) available to access for direct patient care – the Connecting your Care (CyC) project. A full Data Privacy Impact Assessment was also created.

Under the Corona Virus 2020 Act and its Control of Patient Information Notice (COPI), HIE controllers across London connected their HIE’s to provide access to Acute and GP information for direct care purposes across the whole of London. This allows citizens of London to receive timely care no matter where or at what time they sought medical assistance. The COPI Notice, originally for six months has now been extended to the end of March 2022

**Data Privacy Impact Assessments (DPIAs)**

Under GDPR, Data Privacy Impact Assessments became mandatory for high-risk processing of personal information. This is part of the Privacy by Design ethos. The Trust had previously been using DPIAs where new technologies were introduced and they are becoming commonplace for the Trust as we mostly deal with health information, which is a special category of information (similar to DPA 1998 sensitive data) under GDPR. We currently use a tool agreed by the South West London Information Governance Group.

For the purposes of COPI, a short form DPIA was also developed. The lawful basis for all of the COPI DPIA is our public task for health care purposes, and 78 of these DPIAs have been created and approved from March 2020 onwards. For the purposes likely to extend beyond COPI, long form DPIA – which are much more detailed – are underway; for instance, for virtual clinic appointments and the use of MS Teams. It is, however, expected that some of the purposes will be stood down following the pandemic.

**Statutory Requirements**

The Trust fulfils its Caldicott provisions in a number of ways. It has been a signatory to a range of Information Sharing Protocols. The Trust has worked with the South West London IG Group

to provide an Overarching Information Sharing Protocol and Purpose Specific Information Sharing Agreement for the Connecting your Care project, which shares information for direct care between health and social care organisations across South West London. This includes the four acute trusts, mental health trusts, adult social care, GP practices, pharmacies (pilot) and care homes (pilot). The Overarching Information Sharing Agreement and Purpose Specific Information Sharing Agreement are based on the Trust templates. We also collaborated in a Data Privacy Impact Assessment for the project. These are all hosted on the Data Controller Console by the Trust and at the time of writing, 211 organisations had signed up. There have been no incidents which required the intervention of the Medical Director in their capacity as Caldicott Guardian.

Our Purpose Specific Information Sharing Agreement (PSISA) template has also been used for a number of other projects across the Trust and has been adopted by other Trusts as well. We have also developed a template for Data Privacy Impact Assessments, and these are in use for high-risk processing.

### 3. Governance of Information Governance and Key People

The Information Governance Committee is the key governance group overseeing the Trust's information governance activities. It reports into Executive Management Committee (EMC) and is chaired by the Chief Financial Officer (CFO) in her capacity as the Trust SIRO. Amongst other members is the Trust Medical Director who is the Trust Caldicott Guardian.

During 2020/21, the Information Governance Committee met on only two occasions: 14<sup>th</sup> September and 23<sup>rd</sup> November 2020. This was due to a number of committee and board meetings being either stood down or streamlined as a response to the significant pressures caused by the Covid-19 pandemic. In March 2021, although the Committee did not formally meet, it exercised chairs actions in order to approve a number of policies and procedures.

Quorum for meetings is four members, and all meetings in 2020-21 were quorate.

The following table lists the members of the committee by job title and the number of meetings they attended during the year.

<b>Position</b>	<b>Attended</b>	<b>Out of Possible</b>
Director of Finance/SIRO (Chair)	2	2
Medical Director/Caldicott Guardian	0	2
Director of IM&T	2	2
Deputy Director of IM&T (IT Installation Security Officer)	2	2
Head of Business Intelligence (or Deputy)	2	2
Nursing Representative	0	2
Workforce Representative	1	2
Service Manager Cluster 3	1	2
Director of Corporate Governance	2	2
Emergency Planning Manager (or deputy)	1	2
Head of Procurement	1	2
Information Governance Manager	2	2
Head of Information Governance - Secretary	2	2

The Information Governance Committee reported to the EMC by exception during 2020/21. The terms of reference for the Information Governance Committee were reviewed and approved, unchanged, by EMC during the year.

## Policies

The Trust has information governance policies and procedures available through the Intranet under the Clinical Guidelines and Trust Policies Button. These are reviewed every three years as a minimum. Policies and procedures are approved through the Information Governance Committee and ratified by EMC.

The following policies were approved by the Committee during the year:

- National Data Opt-Out Policy
- Data Protection Policy

## 4. Significant Risks Identified and Actions Taken

### Serious Incidents Requiring Investigation (SIRIs)

A report listing Information Security incidents is prepared for the IG Committee by the Head of Information Governance. The information is gathered from the Ulysses Safeguard System. Incidents are also brought to the attention of the SIRO and Caldicott Guardian outside of the Committee by the Head of Information Governance when required. IG Serious Incidents Requiring Investigation (SIRIs) are first logged as Incidents or Complaints on Ulysses then, if required, logged through the Incident Reporting Tool on the DSP Toolkit. Incidents of significant severity are automatically notified to the Information Commissioner's Office. All SIRI's undergo full investigation and root cause analysis, and are then reported to the Information Governance Committee.

In 2020/21 there was one Serious Incident Requiring Investigation (IG SIRIs) through the Data Security and Protection Toolkit . This was further reported to the ICO which, upon investigation, involved a rogue employee of a sub-contractor acting outside the remit of their employer, and was consequently de-escalated.

### Information Governance Risk Register

There are three risks on the IG Risk Register. All are being managed on an ongoing basis. They range from moderate to high risk in scale:

1. Risk of fines from Information Commissioner's Office for breaches of Data Protection Act – **Moderate Risk**
2. Risk of Actions/Fines from Information Commissioner's Office for breaches where there is inadequate DPIA for high-risk processing - **Moderate Risk**
3. Risk to rating on the DSPToolkit and increased risk of IG breaches caused by staff not being up to date in Data Security and Protection Training – **high risk**

## 5. Objectives / Forward Plans

### Electronic Document Management System (EDM)

The Trust has been working on how to digitise it's paper health records over that last two years, including the 2020/21 period. Tenders were placed as two lots under OJEU – for a scanning bureau and for an EDM system to house the records. In late 2021 the Trust deployed the EDM to the early adopted department – Colposcopy. The Project scans the active records as full colour pdf's as the patients are coming up for appointments or elective inpatient activity and these are housed in MediVeiwier which is accessed through our Electronic Patient Record. A system of Slim Files is in place for both inpatient and outpatient where documenting onto paper, rather that direct to our Electronic Patient Record (CRS), is required. The Slim Files are scanned and injected to the EDM. This will improve the availability of records for clinical use and improve patient experience.

In time, the EDM should also facilitate improvement to the Subject Access Request (SAR) process as the paper records can be scanned faster and to greater quality than photocopying. In addition, Subject Access Team Staff do not physically have to move SAR bundles to and from Consultant for consent to release the records.

### **UK Patent Portal**

The Trust is currently working with our Electronic Patient Record supplier (Cerner) and with their subcontractor (Zesty) to create a patient portal where patients can get their appointment letters and reminders and to be able to amend up-coming appointments. At a future stage, patients should have access to their Electronic Patient Record.

**Data Security and Protection Toolkit** – Version 4 of the Toolkit has been launched and there have been very few changes from version 3. Version 4 will be formally BaseLined at the end of February 2022 and Final Submission at the end of June 2022. IM&T secured funding for three out of four projects (covering multiple Assertions in the Toolkit) to aid in gaining Standards Met on the Toolkit. We are investigating ways to bring Training Compliance to 95%.

### **Freedom of Information requests**

Each FOI request must be handled individually and requirements in terms of time and resources can vary considerably, as can the number of requests the Trust receives during a year. Compliance with the 20-working-day statutory limit is still a Key Performance Indicator (KPI), and where possible in the department, we will re-use information acquired through previous FOIs. We are planning to work with colleagues to publish information that is, and may be, the subject of frequent requests, which should cut back on the number of FOIs the Trust needs to respond to. It is also hoped that new staffing arrangements will improve performance over the course of the year, however some of this may be dependent on the resilience of the Trust overall as the pandemic continues.

### **GDPR/Data Protection Act Subject Access Requests**

Our focus is to complete the backlog and achieve compliance with the 28-calendar-day timeframe for the IG Subject Access Team. We are seeking to expand the Team on a temporary basis until EDM is fully deployed. We will also monitor compliance with other major recipients of requests in the Trust. The Head of Information Governance as Data Protection Officer for the Trust continues to deal with any complex issues.

GDPR has expanded the range of information available to data subjects compared to previous years. It is expected that more applicants will request these newly included types of information, such as emails, texts and information in MS Teams channels. The Head of Information Governance also ensures DPA Notification and the updating and publication of the Trusts Privacy Notice.

### **P2 Sentinel and HIE Reporting Tool**

The tool is available to the Head of Information Governance and the Caldicott Guardian as well as key staff in Information Services and IM&T. P2 Sentinel is the Privacy Office/Caldicott Guardian audit tool for CRS Cerner Millennium. It has been used by the Head of Information Governance to investigate incidents at the behest of Complaints, HR, Risk Management and Departments as well as patients.

### **IG Walkabouts**

The IG Team will re-establish the IG Walkabout audits which have not been possible in the Trust due to Covid-19, when this is allowable under the IPC guidelines. Issues found are documented on a control sheet and are mitigated as much as possible at the time. The issues will also be logged onto RLDatix Incident Reporting, and may also need to be added to the Risk Register of the specific departments.

### **CRS (EPR - Cerner Millennium)**

The roll out of Clinical Documentation and E-Prescribing, documenting directly into the system rather than in paper records, continues to proceed and is completed across inpatient areas. Outpatients remains the focus for rollout. This is part of the overall plan to make CRS the patient record, and for the Trust to be paper-light. The system itself continues to be developed to prevent data entry/data quality errors. BigHand Digital Dictation where patient letters are digitally recorded, transcribed as Word Documents, approved by the clinician, then stored in the patient's CRS record as well as an electronic copy going directly by GP Link to the GP's own system, is now well embedded within the Trust.

### **GDPR**

The General Data Protection Regulations (GDPR) came into effect on 25 May 2018 along with the Data Protection Act 2018. The GDPR Data Protection Officer role has been incorporated into the job description of the Head of Information Governance. The Fair Processing Notice, the "Your Information" booklet, has been updated to a GDPR compliant Privacy Notice and this has been published on the Trust Website. The main areas which have changed

- Sharing health information for Direct Care no longer relies on consent but is conducted through our responsibilities under the Health and Social Care Act and for Medical Purposes.
- Subject Access Requests are now Free of Charge unless manifestly unfounded, excessive or repetitive and that the legal time frame is reduced to one month (the Trust has standardized this as 28 days).
- The cost of Data Protection Notification is £2900. This is mandatory.
- Data breaches must be reported within 72 hours. For the Trust this is through the Data Security and Protection Toolkit with automatic notification to the ICO if certain criteria are met
- Data Privacy Impact Assessments are mandatory for high risk processing.

A government consultation has been launched (September 2021) requesting input for a revised Data Protection Act in the UK. It is possible that the UK may well diverge from GDPR which may cancel Adequacy Decision for sharing information with the EEA. Part of the consultation is about re-introduction of Fees for SARs, removing the role of the Data Protection Officer and the need for Data Protection Impact Assessments. Also for consideration is the use of NHS patient information for Public Health Management.

## **6. Conclusion**

It has been a very busy and challenging year for the Trust IG, however the team has continued to contribute to the wider SWL agenda, as well as reorganizing the team and working to ensure business as usual for SARs and FOIs. Although not mentioned in the report, the Trust will be working to have the IG collaborate further with IG at HRCH as part of the Better Together programme.